

ICS 43.040



**NATIONAL STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GB/T 43267-2023

Road vehicles - Safety of the intended functionality

道路车辆 预期功能安全

(English Translation)

Issued on: November 27, 2023

Implemented on: November 27, 2023

Issued by: State Administration for Market Regulation

Table of Contents

Foreword...	5
Introduction...	8
1 Scope...	11
2 Normative references...	12
3 Terms and definitions...	12
4 Overview and organization of SOTIF activities...	26
4.1 General...	26
4.2 SOTIF principles...	26
4.3 Use of this document...	32
4.4 Management of SOTIF activities and supporting processes...	35
5 Specification and design...	37
5.1 Objectives...	37
5.2 Specification of the functionality and considerations for the design...	38
5.3 System design and architecture considerations...	40
5.4 Performance insufficiencies and countermeasures considerations...	41
5.5 Work products...	43
6 Identification and evaluation of hazards...	43
6.1 Objectives...	43
6.2 General...	44
6.3 Hazard identification...	44
6.4 Risk evaluation...	47
6.5 Specification of acceptance criteria for the residual risk...	49
6.6 Work products...	50

Foreword

This document was drafted in accordance with the rules provided in GB/T 1.1-2020

Directives for standardization - Part 1.Rules for the structure and drafting of
standardizing documents.

This document modifies using ISO 21448.2022 Road vehicles - Safety of the intended
functionality.

Compared with ISO 21448.2022, this document makes the following structural adjustments.

- Figures 2 ~ 17 correspond to Figures 1 ~ 16 in ISO 21448.2022;
- Tables B.7 ~ B.15 correspond to Tables B.6 ~ B.14 in ISO 21448.2022.

The technical differences between this document and ISO 21448.2022 and their reasons are as follows.

- Replace ISO 26262-1 with the normatively referenced GB/T 34590.1 ~ 34590.12-

2022 to adapt to the technical conditions in our country;

- Change the definition of the term "acceptance criterion" (see 3.1) to make it easier to understand the term;
- Add the term "priority subset" and its definition (see 3.35) to help support SOTIF analysis, verification and validation, as well as evaluation activities to deal with a large number of scenarios and use cases;
- Add description about Annex E (see 4.3.1);
- Change methods for deriving verification and validation activities (see Table 6).

This document also makes the following editorial modifications.

- Add Note 2, Example 3, Note 3 and Note 4 to the definition of the term "acceptance criterion" (see 3.1);
- Remove some notes in ISO 21448.2022, i.e., Note of the terms "DDT fallback" and "fallback ready user"; Note 2 of the terms "dynamic driving task; DDT", "levels of driving automation" and "scenario"; Note 3 of the terms "minimal risk condition; MRC" and "use case"; Note 2 and Note 4 of the term "operational design domain; ODD"; Note 4 of the term "scene"; as well as description of the source of the terms "hazard", "object and event detection and response; OEDR", "risk" and "unreasonable risk";
- Add Note 3 to the specification of the functionality and considerations for the design (see 5.2);
- Add Notes 4 ~ 7 to the risk evaluation (see 6.4) to facilitate understanding of the

acceptance criterion;

- Add Note 5 on acceptance criteria in the specification of acceptance criteria for the residual risk (see 6.5), which helps to apply and understand how to define risk acceptance criteria based on traffic data analysis;
- Add Note 3 to the objectives of identification and evaluation of potential functional insufficiencies and potential triggering conditions (see 7.1) to help apply and improve the acceptance criteria;
- Remove the note of the example in A.3 of ISO 21448:2022;
- Add Note 4 regarding the content of D.5 (see 7.3.3);
- Change Note 3 of the specification of integration and testing (see 9.3);
- Add Note 6 to SOTIF issue evaluation and resolution process (see 13.4);
- Add simplified examples of specification and design (see A.4) to facilitate understanding and application;
- Add examples of scenario priority subsets based on quantitative rules (see Table B.6) to facilitate understanding and application;
- Add perception system performance target quantification and examples of common sensor performance limitations (see D.5) to facilitate understanding and application;
- Add SOTIF considerations for OTA updates (see D.6), which helps SOTIF consideration during operation;
- Add examples of risk acceptance criteria for autonomous driving systems (see Annex E) to facilitate the application and improvement of the acceptance criteria.

1 Scope

This document provides a general argument framework and guidance on measures to ensure the safety of the intended functionality (SOTIF), which is the absence of unreasonable risk due to a hazard caused by functional insufficiencies, i.e..

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

3 Terms and definitions

For the purposes of this document, the terms and definitions given in GB/T 34590.1-

4 Overview and organization of SOTIF activities

The main objective of this document is to describe the activities and rationale used to ensure that the risk level associated with all identified SOTIF-related hazardous events is sufficiently low.

5 Specification and design

The specification and design can include various aspects as listed in this subclause. Some aspects are relevant only for a specific automation level or a specific implementation. In addition, some aspects are relevant for the specification of the functionality on the vehicle level and some on the element level.

6 Identification and evaluation of hazards

The potential functional insufficiencies and triggering conditions are systematically analyzed. This analysis can consider field experience and knowledge gained from similar projects or experts. This analysis can be conducted in parallel, starting from both.

8 Functional modifications addressing SOTIF-related risks

Measures for handing over authority from a system to the driver are aimed at increasing controllability at lower levels of driving automation. These measures can include, but are not limited to.

The input information for "Specification and design" is updated based on the